Economic Impacts of Rules-based versus Risk-based Cybersecurity Regulations in Critical Infrastructure Providers (Bulk Electricity Providers)[i]

Fabio Massacci (IEEE Member), Raminder Ruprai, Matthew Collinson, Julian Williams

Abstract:

Policy makers are currently proposing new regulatory mechanisms to enhance the security of critical national infrastructure operators. The key question in this scenario is *which is the right way to regulate the cybersecurity of critical infrastructure operators in charge of electricity transmission*? Should optimal cybersecurity regulation follow a US style, mostly 'rules-based' model, or the European and in particular UK approach, which is mostly a 'risk-based', from the perspective of the firm, or a savvier balance of both?

We discuss the economic issues behind this choice and present a cyber-security economics model for public policy in presence of strategic attackers. We have calibrated these models in the field with the support of National Grid, the main operator in the UK and one of the largest operators on the East Coast of US. The model(shows that phase transitions for optimal choices are present: e.g. when incentives have a given combination operators will stop investing in their own risk assessment and only care about compliance (and viceversa). It suggest that different approaches may be appropriate to different conditions (e.g. number of operators and the ability to audit), and that just pushing for more rules may have unintended consequences.

1. Introduction

Incidents of Cyber-crime are typically associated with fraudulent activities exploiting the (in)security of credit card payment schemes or on-line transactions[1]. When these occurrences have affected individual citizens it has been normally attributed to the effort of criminal hackers who infect millions of computers for the purpose of gaining access to information relating to personal financial assets.[2] [3] Over time, the victims may change, but the general modality of the crime, monetization by manipulation of transactions, is inherently similar.

Attacks on *Critical National Infrastructure* (CNI) did not have a specific modality attached to them, at least publicly. This changed in 2009 with the deployment of the Stuxnet malware. Targeted attacks from nation states and criminal organizations have subsequently become more common; or at least more widely reported in as being persistent. These activities, often termed Advanced Persistent Threats, have affected many CNIs from aviation to water processing utilities. Energy operators are not exempt and TABLE 1 illustrates some examples of recent recorded attacks.

The increasing number of cybersecurity issues has now spurred the attention of public policy makers. The US Federal Government (Executive Order 13636) has put forward regulations aimed at protecting the cybersecurity of CNIs and translated them into a substantive technical framework[4]. The European Union has followed suit with a proposal for a specific European Directive in this area.

[i] Authors Affiliation:
- Fabio Massacci is with the University of Trento (IT). Contact at Fabio.Massacci@unitn.it
- Matthew Collinson is with the University of Abderdeen (UK).
- Raminder Ruprai is with National Grid (UK).
- Julian Williams is at Durham University (UK).

TABLE 1 - Examples of Cyber Attack to Energy Providers

Name	Target	Details
Stuxnet	Damage	Bespoke sophisticated malware targeting the nuclear enrichment plants in Iran.
Duqu	Exfiltration	Targeted malware used to infiltrate and extract key pieces of information about ICS for the purposes of reconnaissance.
Shamoon	Damage and exfiltration	A virus used to exfiltrate data from a host machine before deleting the computer's master-boot-record to render the computer useless. Shamoon was used to attack the oil company Saudi-Aramco where 30,000 of it's desktops were infected and subsequently knocked out as the virus took hold.
Havex, Energetic Bear, Dragonfly	Exfiltration	Focussed malware targeting ICS/SCADA systems in the energy sector for the purposes of exfiltrating data for cyber espionage and/or possible use in a future cyber attack.
Regin	Exfiltration	Sophisticated malware designed to target and collect intelligence within the infected systems for use by nation states.

Managing and regulating cybersecurity issues is particularly relevant for *CNI Operators* (CNIOs), private or publicly traded enterprises in charge of the bulk transmission of electricity, oil- production and processing or gas- production and distribution.

Hence, a natural research question arises: "*which is the best way to regulate the cybersecurity of CNI providers*?" As with most important questions, the answer is not straightforward. To answer this question a useful conceptual distinction focuses on who is responsible for the choice of security measures.

At one extreme, which we refer to as a "*rules-based regulations",* the policy maker mandates security provisions for CNIOs by detailed compliance requirements and introduce penalties for non-compliance with those requirements. On the opposite side, referred to as "*risk-based regulations*", the policy maker intervenes with fines consequential to security breaches but let firms define security investments based on their investment profile, their own risk assessment analysis, and the potential losses (including ultimately the loss of license to operate). As an illustrative example, in a pure rules-based system only the policy-maker performs the risk assessment (possibly after a consultation as a US NERC type system for interstate bulk transmission), casts security measures into low-level rules and audits their implementation by CNIOs, fining them for non-compliance. If all rules are met but a breach nonetheless occurs CNIOs are not liable. In a pure risk-based system, the CNIO itself is responsible for performing a risk assessment, deciding the low level countermeasures, and it is not audited. Instead, penalties, are imposed in the event of a successful attack that causes disruptions (the UK regulatory system works in the this fashion).

Real-world regulations are normally "hybrid" between the two extremes and the operational implementation of security controls by a CNIO is a function of the risk environment and the actual regulations.

During the SECONOMICS project (http://www.seconomics.org), we have developed a number of cyber-security public-policy models that capture explicitly the hybrid nature of regulations oscillating between risk-based and rules-based systems. We have calibrated and validated our regulatory models in the field with the support of National Grid, the electricity provider in the UK and in part of the East Cost of the US. The key feature of the model is that we can determine whether a rules-based or a risk-based regulation obtain the best social optimum for the public policy makers, even under the assumption that CNIOs pursue their own commercial interests as privately own companies.

From our parametric specification, the model predicts that substantial variations in the regulatory system maybe appropriate to different conditions. For instance, the number of operators, the effectiveness of audits, the appropriateness of requirements by the policy maker and the cost of attacks all influence the optimal outcome. What is particularly interesting is a qualitative phenomenon: the presence of *discrete phase transitions*. Different types of incentives by the regulator dramatically shift the behaviour of CNIOs and not necessarily in the anticipated manner.

2. Challenges in CNI Cyber Security

CNIOs have a variety of assets with differing levels of criticality to the ongoing functionality and profitability of their operations. In the case of electricity transmission, the critical assets for service could include the energy management system and software and essential operational technology in the field such as local substation control systems. Critical systems that include Supervisory Control and Data Acquisition (SCADA) systems and Industrial Control Systems (ICS). ICS and SCADA systems control the core (critical) functions and operations that CNIOs are responsible for. The role of SCADA systems is to take information from multiple remote sensors/stations and fed it into a central control room where the operators have full visibility of the entire network being managed. The ICS is then linked to the SCADA system through both automated and manual control where actions and control changes can be made from the information that is collated and organised from the SCADA system. Examples of ICS and SCADA systems include electricity and gas management systems run by the transmission grid operators, such as National Grid or a city's train metro control system, such as the London Underground. Over recent years, the cyber security agenda in ICS/SCADA systems has gained greater traction. TABLE 2 illustrate examples of new initiatives over traditional IT Security.

TABLE 2 - Examples of Specific Initiatives in CNI Cyber Security

Acronym	Type	Details
ISA/IEC 62443	Specific Standard	International Society of Automation (ISA)/ International Electro-technical Commission (IEC) standards on the cyber security of industry automation and control systems
GICSP	Professional certification	Certification in Global Industrial Cyber Security Professional
SCSIE	Information Exchange	UK's Centre for the Protection of National Infrastructure (CPNI) SCADA and Controls Systems Information Exchange

The number of high-profile incidents we have listed in TABLE 1 have helped to sharpen the senses of security teams in CNIOs and their Boards. The Stuxnet incident was the first major cyber attack to an ICS/SCADA system. Stuxnet was a piece of bespoke malware, targeted at Iran's Nuclear programme. Its specific purpose was to corrupt the Siemens' SIMATIC WinCC SCADA system that was used to control the centrifuges. A key feature of the Stuxnet malware was its ability to intercept and then alter sensor readings from the centrifuges to the control room and commands being sent back without the operators realising that anything untoward had occurred. This resulted in the malfunction of the centrifuges and batches of uranium being ruined which was the ultimate goal of the attack.

Stuxnet-like malware are highly dangerous, because they are capable of both affecting computer systems across a network *and* they are capable of causing physical damage to critical equipment through attacking the ICS and SCADA systems directly. Further, ICS and SCADA systems traditionally have a far longer lifecycle (15-20 years) than standard IT

equipment. As a result, these legacy systems were often built at a time when information/cyber security was not considered as an important corporate issue. Even today ICS and SCADA vendors are still relatively security immature, which makes securing the systems a difficult proposition for the CNIOs.[5]

There are other assets that might need to be secured, as in other industries, by they are not essential to the critical service and can be categorized as supporting the functioning of that service, often with the goal of ensuring the service is profitably managed (even in the case of state provided transmission systems). For example, users' laptops and HR and finance systems and their applications are not critical to transmission, but ensure that the service is efficiently managed.

Regulators have realized that the security of CNI systems is not at the level of security maturity where they would want them to be (e.g. see ENISA's recent report[6]) but have often difficulty in fully comprehending and appreciating the challenges CNIOs have to overcome in securing the legacy ICS and SCADA systems.

Further, major economics drivers create additional obstacles. In the EU, CNIOs are heavily *price regulated* often due to the monopolistic (or oligopolistic) nature of the energy transmission industry. Therefore, it can be difficult for CNIOs to justify significant security budgets to a regulator that is tasked with keeping prices as low as possible. In the US, *price competition* over a compliance target between a large number of operators returns essentially the same effect. This is one of the key reasons as to why cyber security budgets in many CNIOs are not as high as other similarly sized commercial organizations and maybe inadequate to properly secure ICS and SCADA systems.

As a final challenge is there is also significant variation amongst contemporary security regulations which span the entire spectrum from risk-based to rule-based regimes, set in place by national governments.

3. Different Approaches to CNI Cybersecurity Regulations

Should CNI Operators (CNIOs for short) in charge of electricity transmission be regulated based on risk-based regime or a rule-base regime? The public policy implications of this question cross the Atlantic: should an optimal cybersecurity regulation follow the US, rule-based model, or the UK, risk-based model? Which market conditions or which attacker model justifies one choice over the other or suggests a mixture of both?

In the US, National Grid, for interstate bulk electricity transmission, is required to adhere to a rules-based system for security, run by the North American Electric Reliability Corporation (NERC). NERC is an independent organisation that provides guidelines and standards for electricity transmission operators in North America and enforces reliability standards on electricity transmission operators in the US on behalf of the Federal Energy Regulatory Commission (FERC). NERC monitors the status of various elements of the power distribution system (including cyber security assets). The standards which focus on information/cyber security as well as the CNI aspects of electricity transmission are the Critical Infrastructure Protection (CIP) reliability standards. Each regulated entity has to provide compliance reports against the CIP standard on a yearly basis and is audited every three years. The first CIP standard mandating asset identification (CIP-002 v1) was drafted in 2006. Version 2 went into force in 2010.

In contrast, the majority of cyber security regulation in CNI industries across Europe is not compliance-based. In the UK, National Grid holds a licence to transmit electricity that is

granted by the UK government's Department for Energy and Climate Change (DECC). The headline duty of the transmission licence holder within the Electricity Act of 1989 states that

"*It shall be the duty of the holder of a licence authorising him to transmit electricity to develop and maintain an efficient, co-ordinated and economical system of electricity transmission[…]*."

The Electricity Act does not specifically require the licence holder to be "secure", but not having the relevant cyber security controls in place may jeopardise the electricity transmission in case of cyber-attacks and therefore the licence itself. The operator is then free to decide how they will ensure they are cyber-secure. The regulation is risk-based.

Looking beyond the regulatory environments in the UK and US, TABLE 3 illustrates the difference in regulations between some countries in Europe and USA that we obtained from a survey of the cybersecurity group members of ENTSO-E (European Network of Transmission System Operators for Electricity).

TABLE 3 – Regulatory Regime in Different Countries

Type of Regulation	**Applicable Countries**
Mostly risk-based	Belgium, France, Italy, Netherlands, Switzerland, United Kingdom
Risk-based with some rules-based	Austria, Poland, Germany
Rules-based with some risk-based	France
Mostly rules-based	USA

Regimes can change over time. As an example, the German regulatory system for security of critical industries like electricity transmission is currently based on high-level principles. The German Federal Ministry for the Interior will be establishing a requirement for utilities to obtain an ISO27001 certification (a security standard). Part of the new regulation includes security audits and the 'right to inspect' by the regulator. Whilst the ISO27001 standard includes a risk management framework, several security controls are effectively mandatory. These can be viewed as specific rules in addition to the headline rule to be certified to that standard. This is a jump from a mainly risk-based to a mainly rules-based regulatory system.

In an additional example of the changing regulatory landscape, the European Commission has put forward the European Network and Information Security (NIS) directive[6] to ensure that CNIOs meet appropriate IT security standards, share information about threats, report incidents an security breaches in a consistent manner across Europe. The proposed mandatory requirements within the NIS directive have been received with the full spectrum of responses because cyber security maturity varies widely in the different EU member states. Some are in favour of the directive, as it would aid in pushing CNIOs to do more in security thereby increasing their overall security maturity. Other EU member countries have concerns that the compliance-based nature of the directive could stall existing good relationships between governments and CNIOs. For instance, requirements for mandatory incident reporting may drive CNIOs to hide/tone down security events for fear of further repercussions or reputational consequences.

National Grid owns and operates the UK's electricity and gas transmission networks and provides gas distribution for around half of the UK. National Grid also owns and operates electricity and gas transmission networks, as well as distribution networks, in a significant proportion of the North Eastern United States. Due to this coverage of providing utility delivery services in the UK and US National Grid Security function deals with every aspect of

both, diametrically opposed, regulatory regimes. Therefore, this has provided a fruitful case study opportunity in analysing the risk versus rules based regulatory mechanisms.

4. Current Security Economics Models don't apply to CNI scenarios

Traditional security economics models have captured attacker—target interactions as Bayesian games, early work that builds on the 'weakest link' game have predominated in this area[7]. Fultz and Grossklags[8] use the classic paradigm of defenders and attackers, playing a one period game under various assumptions for the attacker objectives and constraints on the defenders technology and actions. Earlier papers use a slightly simplified model of attack and defense to determine the optimal allocation of liability to vendors for software patching[9]. A similar, single period game elucidates the optimal policy for software vulnerability disclosures[10]. The behavioral aspects of attacker-target interactions can also determine how much information is optimal to share[11].

Why is it important to differentiate between CNI firms, which are regulated in some manner, and those in other less regulated sectors such as technology and retail? The answer lies primarily in the systemic risk that accompanies the 'critical good' that the CNIO is providing.

At first, there is usually *one* bulk electricity transmitter for a European country (or a US or Canadian state) as the geographical spacing restricts competition. Second, CNIOs are now run as `normal' firms, often quoted in the stock exchange and thus run with the same overarching objective as any other firm: maximizing the present value of shareholders interest. Corporate officers who make decisions for a firm would be expected to exhibit risk-aversion in acting for themselves[12] but the theory of the firm suggests that corporate officers should act on behalf of their shareholders[13]. We end with a risk-neutral, rent seeking, monopolist in charge of a risky, critical service for the society. Therefore, to avoid the exploitation of its own citizens, a government agency normally regulates in some way the degree of investments made by the CNIO and limits the charges paid by customers. The `price cap' model is a UK system that sets a maximum cost of the good. An alternative model, used in the USA, is a `rate-of-return' regulation that limits utilities to a maximum rate-of-return on capital for investors.

This complicates the standard attack-defense game in several directions. At first, unlike in the standard target firm versus attackers, the major costs of successful attacks are often not fully borne by the CNIO, but by the public at large. To ensure that the CNIO properly invests in security provision the policy makers need to balance (i) the resources that they allow the operator to extract from the consumers, (ii) the minimal mandated and audited investment, and (iii) the penalties and fines for poor service (e.g. in the event of a successful attack).

Second, given the privatized status of the CNIO form, any transfer from a 'rate setting arrangement' will be invested to provide the maximum expected surplus for the shareholders subject to future risk outcomes. Divergent opinions on the likelihood and impact of future successful attacks will lead to a tension between the policy maker and the CNIO on resource allocation. For example, if the regulator is uninformed on the costs of security and is convinced by the operator to have a large transfer, but then caps the transfer to shareholders, the operator will act in an inefficient manner (the Averch-Johnson effect[14]).

Finally, finding the appropriate discount rate for future losses in electricity transmission may face the same problems discussed in environmental economics and in the economics of climate change. Larger scale ecosystems (such as the Internet or long distance electricity grid) are usually assumed to require longer term planning (and therefore low discount rate). The social planner may desire the risk externalities of bulk electricity transmission to be managed over a longer, more sustainable, time horizon, then his discount rate will be set

lower than the normal rate of return of investments determined by a market-driven CNIO. Each participants in the ecosystem will therefore struggle against the costs for amortization of risk they believe to be unfair given their own time preferences.

Understanding the security economics of defenders-attackers interaction in such (semi)regulated environments is therefore critical.

5. A Game-theoretic Model of Subsidies and Incentives

To tell regulatory systems apart from a sound conceptual perspective, we introduce the Institutional Analysis and Development (IAD) model suggested by Crawford and Ostrom[15]. Similar frameworks with a rigorous mathematical underpinning have also been applied elsewhere[16]. The IAD framework extracts the key features of the institutional design narrative (from the hundreds pages of the NERC/FERC regulations or the several acts of European governments) and from these features a mathematical model based on game theory can be soundly developed.

Crawford and Ostrom introduced the notion of a *policy action arena*, which is the domain of interactions, e.g. the regulation of cyber security. Within the arena we observe *rules*, *norms* and *strategies*. Each macro concept is formally described by a set of refined concepts. An *attribute* (A) is the individual or organization to which the policy institution statement applies. The *deontic* (D) `prescriptive operator' describes what is ideally permitted, obliged or forbidden by the institutional statement. The *aim or intention* (I) describes the goal or action of the statements for which the corresponding deontic refers. The *condition (C)* specifies when and where the aim is appropriate. The *or-else* (O) is the punishment action when a rule is not adhered to. For rules the entire syntax is valid (ADICO), for norms only attribute, deontic, aim and condition apply, (ADIC). Strategies include only attribute, aim and condition (AIC).

The difference between the two regulatory systems is in the entity setting norms and the type of or-else punishments. For *risk-based* systems, the entity contracted for the service determines the specificity of the operational norms whilst the public body sets the over-arching principles with either explicit (ex-post fines for poor or absent service) or implicit (loss of licence) punishments. In a *rules-based* system the public body sets and audits operational norms, determining them from its own principles. Hybrid systems vary in the degree of discretion the service provider has in setting operational norms and the specificity of audit and a-priori fines for breaches of audit, relative to fines for disruption of provision.

To build a model, we assume that the policy-maker is a single coherent decision-maker, as is the CNIO. This is appropriate to characterize monopoly CNI situations, common in EU states and in many US states. Another assumption is that CNIOs are responsive to policy actions, albeit not necessarily in the way the policy maker expects.

A CNIO can decide the level of investment in rules compliance I_{rules} and the level of investment in risk-based security I_{risk}. Intuitively, they are the response to the incentives set-out by the policy maker. These investments are assumed to be separate and to account for all security investments. Thus, compliance investment, whilst it may have the effect of reducing risk, is not by itself classified as contributing to risk-based investment.

The policy-maker set policies represented mathematically as pairs of functions describing the strength of incentives for security rules compliance (the result of failing an audit $failure_{Audit}$) and strength of incentives for risk-based security behaviour (punitive *damages* consequence of successful attacks). The policy-maker has a further action available, being the subsidy S

allocated to the CNIO. The precise form of this subsidy – for example a consumer fee with price or rate-of-return cap, or a direct transfer of funds – is not relevant.

A specific security aspect is the presence of rational adversaries who benfits from security breaches. In some models, breaches are taken to arise stochastically, as though generated by some partially unknown process. In the present model, CNIO and attacker simultaneously anticipate and react to each other's choices, where the attacker needs to choose a level of attacking intensity A.

These actors can be characterized to the following risk neutral utility functions:

$$U_{\text{firm}} = S - I_{rules} - I_{risk} - failure_{Audit}(I_{rules}) - (fines+losses) \times \Pr_{\text{Attacks}}(A, I_{rules}, I_{risk}) \quad (1)$$

$$U_{\text{attacker}} = reward \times \Pr_{\text{Attacks}}(A, I_{rules}, I_{risk}) - A \quad (2)$$

$$U_{\text{policy maker}} = W - S - lack_{assurance}(I_{rules}) - damages \times \Pr_{\text{Attacks}}(A, I_{rules}, I_{risk}) \quad (3)$$

Equation (1) represents firm pay-off and we can see that they receive a subsidy S and expend deterministically investments I_{rules} and I_{risk}. When the firm is audited and is found wanting of a compliance requirement, it receives a fine $failure_{Audit}(I_{rules})$. We assume that this function is hyperbolic: it decreases with I_{rules} but the marginal effectiveness of additional investments decreases for large investments. This assumption is typical for models of choice under uncertainty used in economics from public policy to finance.

This ensures that the firm chooses an optimal level of I_{rules} at a maxima rather than as a boundary condition from an arbitrary budget constraint. For the stochastic loss resulting from the term $(fines+losses) \times \Pr_{\text{Attacks}}(A, I_{rules}, I_{risk})$ we make a similar assumption: the probability of successful attacks is hyperbolic in the plane of I_{rules} and I_{risk} for a given level of A, and is obviously increasing in attacking intensity A. Therefore, success probability decreases with the total amount of investments but the marginal effectiveness of each additional dollar diminishes for large investments. As a consequence, the firm will choose an optimal level of effort I_{risk} and the contribution of random losses to the choice of I_{rules} attains a unique maxima.

Equation (2) represents the pay-off of the attacker. We assume that there is a *reward* and a cost of effort (rolled into the value A). Given the previous assumptions on $\Pr_{\text{Attacks}}(A, I_1, I_2)$ then the also attacker will have an optimal unique intensity for attacks. The major issue arises from a lack of empirical measures of A and *reward*. At present we can only view attacks that have occurred and so we do not know the full set of available attacks or have a measure of their difficulty. However, we can treat the unknown parameters as variables for parameter explorations and this provides us with the policy domains of interest.

Equation (3) presents the policy-makers risk-neutral expected pay-off. The policy maker has a quantity W of wealth and allocates an amount S. The policy maker receives verifiable assurance from the firm by the expenditure of I_{rules} and this level of assurance is proportional to the level of investment by the firm. The $lack_{assurance}(I_{rules})$ captures this effect, as the level of I_{rules} increases then $lack_{assurance}(I_{rules})$ converges to zero; whilst as I_{rules} tends to zero, the term $lack_{assurance}(I_{rules})$ tends to a fixed value that represents the overall concern of the policy-maker in the absence of verifiable information from the firm. Finally, the term $damages \times \Pr_{\text{Attacks}}(A, I_{rules}, I_{risk})$ denoted the expected degree of damage to society from attacks. This term is not directly affected by the policy makers actions, however, it is indirectly affected by the choice of function $failure_{Audit}(I_{rules})$ and the level of *fine(s)* the policy maker imposes on the firm and these are the key policy levers. We denote these levers as *the incentive for risk-based security investment* and the *incentive for rules-based security investment.*

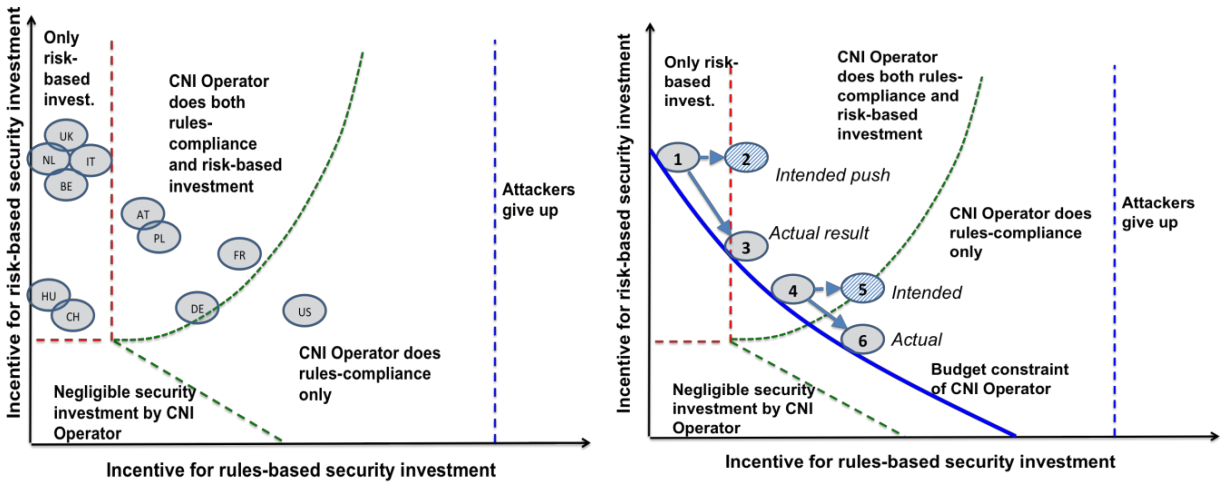
When designing such an attack and defence model, the modeller has to be careful to ensure that the unit of account of each agent (attacker, firm corporate officer and policy-maker) are separately measured. Equations 1 and 3 In the most general specification the common terms (notably the subsidy S and the investments I_{rules} and I_{risk}) will have multipliers in front of them to ensure that the they are evaluated according the unit of account and the level of risk aversion of each actor. For example, the policy maker may values the public subsidy S at the higher rate than the firm receiving it (for instance when it is obtained directly from taxation).

At this stage, a general solution would be to build a complex game with three types of player. Our simpler and effective alternative is to treat the attacker-target interaction as a sub-game with a Nash equilibrium for a given set of incentives. The policy maker will then optimize the incentives considering the solution of the Nash equilibrium. The detailed mathematical representation of the model can be found in SECONOMICS Deliverable D6.4.

6. Policy Implications for Security of CNI Operators

Our models have been built, calibrated and refined in an iterative process through involvement with industry security leaders in the energy sector and there are number of policy implications that stem from this analysis.

The interesting phenomenon is that the choices of incentives by the policy maker divide the policy arena in regions of behaviour for the CNIO and the attackers. **Figure 1**a illustrates our phase diagram. If the incentives for rule-based compliance are massive, the attacker will eventually be priced out (blue line on the right). If the incentive for risk-based self-assessment increases and the incentive for rule-based compliance decreases (eg CNIOs can shirk audits, or the fines are not high enough) then the regulator should switch to risk-based regulatory regimes (the red boundary) so that companies would make their own security risk assessment and invest accordingly. Countries listed in TABLE 2 have been positioned in the plane according to the incentive structure surveyed from the ENTSO-E cybersecurity group.



In each zone CNIOs react differently to incentives. If both are low they do actually nothing. If there is too much emphasis on compliance they only invest in meeting rules. Otherwise they will do a risk assessment and invest to mitigate the critical threats.

Just adding more rules doesn't help: the policy makers would like to push CNIOs from (1) to (2) and from (5) to (6) but since CNIOs only move along the budget constraints the actual effect is that (4) stops doing its security analysis and only cares about compliance (6).

Figure 1 - Phase Regions of CNIOs Behavior Depending in Incentives

Given the presence of the no-attack region, the policy maker would intuitively like to push CNIOs on the right by adding more rules. Unfortunately, the above phase transition diagram must be intersected with the actual financial means of the firm, the solid blue line in **Figure 1**b, often capped by the regulator itself. Therefore, the push for more rules might have unintended consequences: instead of increasing security, the additional rules (eg adding the obligation to meet the NIS Directive to the CNIO in (1), or the additional compliance of NIS *and* ISO27001 for the German operator in (4)) will push them to disinvest in the security measures they identified as critical and potentially down towards the compliance-only region.

The qualitative structure of the phase diagram does not change with model parameters but the precise value of the optimal policy choice, and the budget constraints depend on them. For example, the rate of mitigation returns to investment in rule compliance impacts the position of the green line, so different estimations by the firm and the policy-maker may lead to different expectations of policy outcomes and potentially damaging misunderstandings. Policy-maker and CNIO should have a shared view of the outcome (response by firm and attacker) that arise from the policy.

If we look at US, nearly 400 firms provide bulk electricity transmission services across the continent. Their size varies from large, risk mature, multinational corporations (such as National Grid) to very small firms operating in sparsely populated areas. Such variation determines a corresponding variation in time horizons, risk preferences, and associated investment profiles. Externalities created by underinvestment by individual firms can create sizeable costs for other CNIOs and the wider public. In this instance, NERC-CIP regulations provide state and federal public policy planners a rules-based system designed to provide assurance on minimum levels of cross-sectional protection.

In the EU context, the majority of bulk electricity transmission operators are national entities. The need of a coordinated regulatory regimes NERC-style appears to be fundamentally different as the problem of externalities is smaller in this environment. If the interconnection between European countries, and the number or maturity of operators would change significantly in the future this approach should need to reconsidered.

Below we present some of the high-level reflections stemming from validation meetings:

- The effectiveness of a rules-based regulation depends on how well informed the regulator is of the security of key assets. If IT architectures differ across each organisation it will be difficult for a regulator to precisely state in the regulation which assets are subject to security requirements. So, CNIOs may exploit gaps in the regulation and substitute the use of regulated assets (subject to security rules) with unregulated ones (thus subject to no rule), hence lowering the overall security of the system.
- A regulator's payoff depends on what it values as important. If a regulator values assurance i.e. demonstration of compliance to security rules, their payoff will be higher the more stringent the rules and the audits are. This might be particularly important if the budget constraint is tight and the risk of ending in the no-action zone is high. If regulators value the absence of security incidents to the service provided by the CNIO then making the rules more rigid will only yield a small benefit (See also **Figure 1**b). Therefore, understanding what the regulator or policy maker values from CNIOs is key to the balance between rules-based and risk-based regulation.
- Cultural attitudes vary and this can have a significant impact on how firms and CNIOs react to security regulation, or its absence. In some jurisdictions with a risk-based regulatory system, CNIOs respond in a collaborative manner with the regulator and

government agencies to develop a security posture that all buy into. There are countries where CNIOs and firms in general choose to do very little in security with similar risk-based regulations in place. This is causing regulators to re-evaluate their approach in such countries, particularly in the EU.

Many security leaders involved in this work thought that a mixed regulatory response could be implemented. Specifically, rules could apply to CNIOs that were less security mature and CNIOs above a certain maturity threshold (i.e. those with an established risk management and mitigation framework) would be subject to a risk-based regulatory framework. In this way, the rules-based regulation would bring up less mature organisations above the bar and the risk-based regulation would allow mature organisations to innovate and lead the industry.

Identifying the maturity threshold is an interesting issue for future work.

7. Acknowledgements

This work has been partly funded by the European Union's 7th Framework Programme under grant agreement no 285223 - SECONOMICS (www.seconomics.org).

8. Bibliography

[1] FBI, "*Internet crime report 2012*," Internet Crime Complaint Center, Tech. Rep., 2013

[2] J. Franklin, A. Perrig, V. Paxson, and S. Savage, "An inquiry into the nature and causes of the wealth of internet miscreants," in *Proc. of ACM Conf. on Comp. and Comm. Security (CCS-07),* pp. 375– 388. 2007.

[3] N. Provos, P. Mavrommatis, M. A. Rajab, and F. Monrose, "All your iframes point to us," in *Proceedings of the 17th USENIX Security Symposium*, pp. 1–15. 2008.

[4] National Institute of Standards and Technology. "Framework for Improving Critical Infrastructure Cybersecurity." 2014.

[5] E. Knapp, "*Industrial network security: securing critical infrastructure networks for Smart Grid, SCADA, and other industrial control systems*." Elsevier. 2011.

[6] European Union Agency for Network and Information Security. "Protecting Industrial Control Systems - Recommendations for Europe and Member". 2011

[7] J. Hirshleifer, "From Weakest-Link to Best-Shot: The Voluntary Provision of Public Goods." *Public Choice*, 41(3):371-386.

[8] N. Fultz and J. Grossklags. "Blue versus red: Towards a model of distributed security attacks." In *Proc. of Financial Cryptography and Data Security* (FC'09), pages 167–183. Springer Verlag, LNCS 5628. 2009.

[9] H. Cavusoglu, and J. Zhang. "Security patch management: Share the burden or share the damage." *Management Science 54*(4):657–670. 2008.

[10] A. Arora, R. Telang, and H. Xu. "Optimal policy for software vulnerability disclosure." *Management Science 54*(4):642–656. 2008.

[11] M. Cremonini, and D. Nizovtsev. "Risks and benefits of signalling information system characteristics to strategic attackers. *J. of Management Inf. Sys. 26*(3):241–274. 2010.

[12] T.Baker, and S.J. Griffith. "Predicting Corporate Governance Risk: Evidence from the Directors' and Officers' Liability Insurance Market." *Chicago Law Review*, Vol. 74, p. 487. 2007

[13] J. Tirole. "*The Theory of Industrial Organization*," MIT Press. 1988.

[14] H. Averch, and L. Johnson "Behavior of the Firm Under Regulatory Constraint". *American Economic Review* 52 (5):1052–1069. 1962.

[15] Crawford, S. E. S. and E. Ostrom. "A Grammar of Institutions." *The American Political Science Review*, Vol. 89, No. 3., pp. 582-600. 1995

[16] K. Binmore. "*Natural Justice*." Open University Press. 2011.